UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-0001

AUG 15 2019

Mr. Steve Weis
MuckRock News
DEPT MR 78756
411A Highland Ave
Somerville, MA 02144-2516

Dear Mr. Weis,

This letter is a follow-up to your August 9, 2019 Freedom of Information Act (FOIA) request (Log #DOC-NIST-2019-001948) to the National Institute of Standards and Technology (NIST) in which you requested:

> Any documents related to the choice of elliptic curves over prime fields for ECC key agreement that first appeared in FIPS 186-4 Appendix D, sections D.1.2.1-D.1.2.5 (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf). For example, any information to the choice of D.1.2.3: P-256: SEED = c49d3608 86e70493 6a6678e1 139d26b7 819f7e90.
>
> This document has been superseded by NIST 800-56A (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf).
> Please return any email, memorandum, presentations, reports, articles, research papers, justifying the choice of initialization parameters for the following standards: P-224 (also known as secp224r1), P-256 (secp256r1), P-384 (secp384r1), P-521 (secp521r1) Dr. Jerry (or Gerald) Solinas from the NSA may have been involved in the parameter selection.

For the purpose of the FOIA, it has been determined that you are in the "media" requester category, which means that you will be charged for duplication of responsive documents excluding the cost of the first 100 pages of duplication. Our initial estimate is under the chargeable threshold; therefore, we are proceeding with the search, review and duplication of responsive documents.

Since this is just an estimate, if the actual cost for the duplication of responsive documents is more than the estimate, then we will notify you of the revised charges. Please be advised that charges are assessed whether or not responsive documents are located and whether or not any of these documents are exempt from disclosure under FOIA.

Responsive documents will be forwarded to you on a rolling basis as they become available.

Sincerely,

Catherine S. Fletcher
Freedom of Information Act Officer

NIST